

Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

United States Courts
Southern District of Texas

FILED

January 29, 2020

David J. Bradley, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
4400 Boone Road Apt 144 Houston, TX 77072

Case No. **4:20mj0162**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 USC 841(a)(1)
21 USC 843

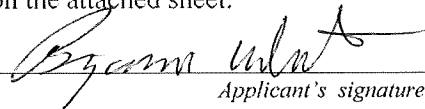
Offense Description
Distribution or possession of a controlled substance with the intent to deliver
Use of Communication Facility in Commission of Drug Trafficking Crime

The application is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Benjamin Whitsitt, Postal Inspector

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: January 29, 2020


Judge's signature

City and state: Houston, Texas

Dena Hanovice Palermo, US Magistrate Judge

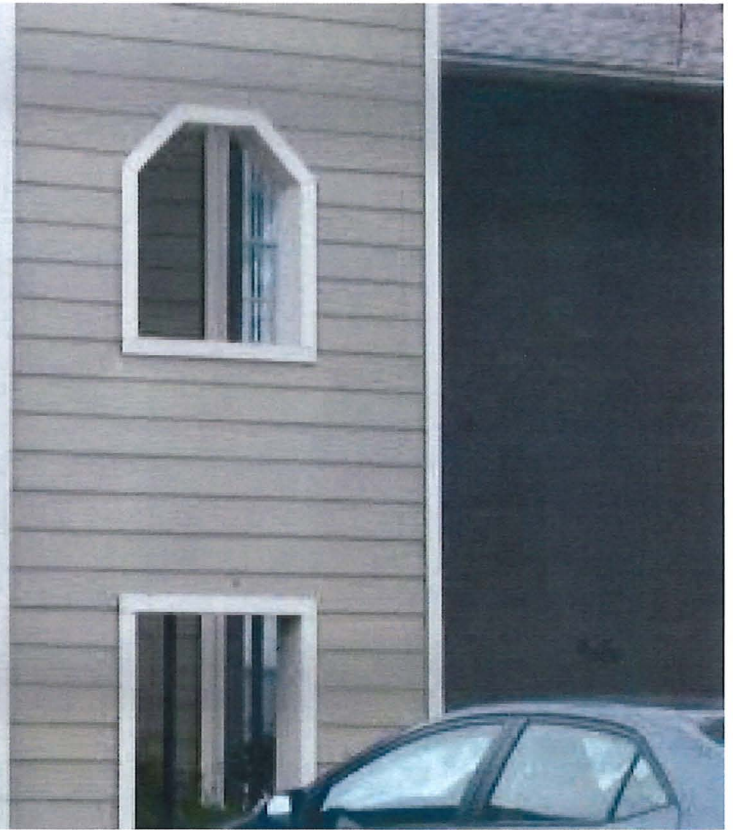
Printed name and title

ATTACHMENT A

The Subject Location is located at 4400 Boone Road Apt 144 Houston, TX 77072. The Subject Location is more particularly identified as an individual apartment located on the 2nd floor of the Brays Village apartment complex, a multi-family apartment complex. The entry door is a dark brown colored door surrounded by a white colored frame. The door handle is on the left side of the door, with inward opening hinges on the right side. The numbers "144" are located on the front of the entry door and door frame. The Subject Location includes all computers and closed and locked containers therein, and all associated outbuildings or storage units.







ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

The following items, located within the Subject Location (together, the “Subject Location”), as described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) & 846 (distribution of controlled substances and conspiracy to distribute controlled substances); Title 21, United States Code, Section 841(h) (dispensing controlled substances via the Internet); Title 21, United States Code, Section 843(b) (illegal use of the mail); Title 18, United States Code, Section 1956 (money laundering) (the “Subject Offenses”), beginning in 2018 and continuing until the present:

1. Controlled substances or derivatives of those controlled substances;
2. Implements and materials used in connection with the manufacture, production, storage, or dispensing of drugs such as postage, packaging material, weight scales, plastic bags, plastic containers, cardboard boxes, mailing envelopes, packaging tapes, labels, label machines, vacuum sealers and cellophane;
3. Books, records, receipts, notes, ledgers, correspondence, and other information relating to the transportation, ordering, purchase, and distribution of controlled substances or proceeds of controlled substances, including customer lists, dealer lists, and contact information for any of these customers and dealers;
4. Articles of personal property tending to establish the identity of the persons in control of the Subject Location and contraband-related paraphernalia located in the Subject Location, such as rent receipts, mail envelopes, photographs, and keys;
5. Information, notes, software, documents, records, or correspondence evidencing violations of the Subject Offenses;
6. Information, records, documents, invoices, and materials that concern any accounts with an Internet Service Provider, email or social media accounts, or other remote computing storage;
7. Information, documents, records, photos, videos, or correspondence that aid in the identification of persons involved in violations of the Subject Offenses;
8. United States or other currency, financial instruments, jewelry, precious metals, and any containers or secret compartments capable of holding the same, that constitute evidence or proceeds of violations of the Subject Offenses;
9. Documents, records, or information relating to the transfer, purchase, sale or disposition of virtual currency.

10. Records and documents pertaining to banking, real estate, or other financial transactions, including the sale of goods, that constitute evidence of or proceeds of the Subject Offenses or the concealment or expenditure of proceeds of the Subject Offenses;
11. Documents related to household expenditures, including but not limited to telephone bills, utility bills, and bills for household items, and the rental of post office or other locations where mail may be received;
12. Indicia of occupancy, residency, rental and/or ownership of the Subject Location, including, utility and telephone bills, canceled envelopes, rental purchase or lease agreements, and keys;
13. Indicia of ownership or control over any vehicles located at the place to be searched, including, but not limited to, titles, registrations, gas receipts, repair bills, and keys belonging to that vehicle;
14. Copies of income tax returns and related correspondence concerning William Wells, and any other entities under the control of these individuals;
15. Travel records, including passports, visas, airline tickets, boarding passes and airline ticket receipts relating to the Subject Offenses;
16. Items used for identification, including identification cards under fictitious names, monikers, and any other type of identifying documents, whether legitimate or fictitious;
17. Records and keys related to self-storage units, post office boxes, commercial mail receiving agency private mail boxes, and safe deposit boxes;
18. Firearms and ammunition;
19. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:
 - a. Routers, modems, and network equipment used to connect computers to the internet;
 - b. Records of Internet Protocol addresses used;
 - c. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.
20. Documents, records, or information relating to email, online, or dark web accounts including:
 - a. Documents, records, or information associated with monikers, usernames, passwords for messaging applications, encrypted messaging application or dark web marketplaces or forums;

- b. Other monikers used in furtherance of the Subject Offenses;
 - c. Documents, records, or information associated with email addresses;
 - d. Documents, records, or information relating to any other email or online accounts used in furtherance of the Subject Offenses;
21. Virtual or digital or cryptocurrency in any format, including but not limited to, wallets (digital and paper), public keys (addresses) and private keys;
22. Any and all hidden services accounts used in furtherance of the offenses described above, including, but not limited to, dark web market accounts, associated dark web forum accounts and Tor-based email accounts.¹;
23. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com² accounts or bitcoin-otc internet relay chat channel³ accounts.
24. Computer(s), digital storage media, or digital storage devices, any physical object upon which computer data can be recorded, computer hardware, computer software, servers, computer related documentation, computer passwords and data security devices, gaming devices, tablets, flash drives, volatile data, digital communications devices, cellular telephones, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected

¹ Hidden services (.onion services) are accessed through the Tor anonymity network. Most are considered dark web services with no legitimate or identified service provider to which legal process may be served.

² LocalBitcoins, OY (and their associated web platform, localbitcoins.com “LBC”) is a Finnish company which is not a licensed money transmitting business registered with the U.S. Government and compliant with the Bank Secrecy Act, which requires establishment and maintenance of anti-money laundering (AML) programs in accordance with know your customer (KYC) rules, such as identifying persons involved in currency transactions over certain thresholds. LBC is not considered a legitimate service provider to which legal process may be served for accurate subscriber information or account seizure.

³ Internet Relay Chat (IRC) is a decentralized chat system which enables people with an installed client (computer program which sends and receives messages to and from an IRC server via the internet) to join in live discussions with anyone else connected in the same manner. The IRC server ensures that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once; each one is assigned a unique channel. One such channel is #bitcoin-otc, in which virtual currency trades are negotiated and arranged. All transactions that may occur are conducted directly between counterparties, without any participation or intermediation from the hosts of IRC servers, and therefore no entity to which legal process may be served for accurate subscriber information, transactional history or account seizure.

devices used for accessing computer storage media that was used to commit or facilitate commissions of the Subject Offenses.

25. For any computer, cellular telephone, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, COMPUTER) that is called for by this warrant, or that might contain items otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, "chat" or instant messaging logs, photographs, and correspondence;
- b. evidence of software that may allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of how and when the COMPUTER was used or accessed to determine the chronological context of computer access, use, and events relating to the Subject Offenses under investigation and to the computer user;
- g. information about usernames or any online accounts or email addresses that include the email accounts and monikers listed in paragraph 20;
- h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- j. contextual information necessary to understand the evidence described in this Attachment B;
- k. volatile data necessary to preserve evidence prior to powering-off and unplugging a running computer;
- l. any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of the Subject Offenses;

m. Items or evidence of items otherwise described above in paragraphs 1-24 of this Attachment B.

26. Executing law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of persons reasonably believed to be the user(s) of the a device onto the Touch ID or fingerprint sensor of any Apple iPhone, iPad, or other Apple brand device, or other device that has a fingerprint sensor, in order to gain access to the contents of any such device. Law enforcement personnel may also depress the fingerprints and/or thumbprints of persons reasonably believed to be the user(s) of the device in order to gain access to applications on the device that may be locked with a fingerprint or thumbprint.

DEFINITIONS:

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Benjamin Whitsitt, a U.S. Postal Inspector currently assigned to the Houston Division's Headquarters of the United States Postal Inspection Service, being duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a United States Postal Inspector and have been so employed since February 2017. I am currently assigned to the United States Postal Inspection Service (USPIS) Houston Division, specifically to the Contraband Interdiction and Investigations team (CI2) in Houston, Texas, which is responsible for investigating narcotics violations involving the United States Mail. My responsibilities include the detection and prevention of the transportation of narcotics/controlled substances through the United States Mail, to include, conducting narcotics investigations and executing arrests of individuals for violations of Title 21, United States Code, Sections 841(a)(1) (Distribution of a Controlled Substance), 843(b) (Use of a Communication Facility to Facilitate the Commission of a Federal Drug Felony), and 846 (Conspiracy to Distribute a Controlled Substance). Part of my training as a Postal Inspector included narcotics trafficking investigative techniques related to the identification and detection of controlled substances being transported in the United States Mail.

2. Prior to joining the inspection service I was employed by the United States Border Patrol for five years and employed as a Dallas Police Officer for six years. During my career as a law enforcement officer, I have worked drug trafficking investigations and participated controlled substance investigations involving the transportation of controlled substances or proceeds/payments through parcel delivery services, to include the United States Mail. During this time I have intercepted or helped in intercepting parcels which were found to have contained

controlled substances or the proceeds of controlled substance sales. I have received training by the U.S. Postal Inspection Service (USPIS) in the investigation of controlled substances or the proceeds of narcotics sales being transported through parcel delivery services.

3. I am a law enforcement officer within the meaning of Section 2510(7) of Title 18, United States Code, and am authorized by law to conduct investigations and make arrests for offenses in Title 18, United States Code, Section 2516. I am a federal law enforcement officer within the meaning of Fed.R.Crim.P. 41(a)(2)(C) and am thus authorized to apply for a search warrant pursuant to this rule.

PURPOSE OF AFFIDAVIT

4. This Affidavit is submitted in support of an application for the issuance of a search warrant for the premises at the following location: 4400 Boone Road, Apartment 144, Houston, TX 77072, as further described in Attachment A (the "Subject Location"), there being probable cause to believe that located in the places described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) & 846 (distribution of controlled substances and conspiracy to distribute controlled substances); Title 21, United States Code, Section 841(h) (dispensing controlled substances via the Internet); Title 21, United States Code, Section 843(b) (illegal use of the mail); Title 18, United States Code, Section 1956 (money laundering) (the "Subject Offenses").

5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses are presently located at the Subject Location.

6. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

PROBABLE CAUSE

7. This investigation targets the dark web vendor STILLSKYHI/deepdreamz/FIENDEMPIRE/HTRAIN (herein after referred to as SSH) and encompasses the activities in violation of the Subject Offenses. This drug trafficker operated online via various dark web marketplaces and a Wickr chat room. The two marketplace vendor accounts operated were FIENDEMPIRE and HTRAIN, while the Wickr chat room operated was deepdreamz. This investigation has revealed that William Wells (“SSH”) is the leaders of an online trafficking organization responsible for the distribution of controlled substances to individuals throughout the United States, via the U.S. Mail. The details set forth below are a summary of the significant aspects of this investigation. Investigators believe evidence pertaining to this long-term drug conspiracy will be found in the Subject Location.

8. The “dark web” is a portion of the Internet, where individuals must use an anonymizing software to access content and websites. Within the dark web, criminal marketplaces operate allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet.

9. “Vendors” are the dark web’s sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of “vendor accounts” on dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor and customer accounts are not identified by numbers, but rather monikers or “handles,” much like the username one would use on a clear web site.

10. The “Tor network,” or simply “Tor” (an abbreviation for “The Onion Router”), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol (“IP”) addresses of the computers accessing the network, and, thereby, the locations and identities of the network’s users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as “hidden services” on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in “.onion” and can only be accessed through specific web browser software, including a browser known as “Tor Browser,” designed to access the Tor network. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user’s cellphone, which then routes the phone’s IP address through different servers all over the world, making it extremely difficult to track.

11. Wickr is a well-known mobile instant messenger application that employs encrypted technology and content messages, including photos, videos, and file attachments that expire after a pre-set time.

12. One common way in which illicit purchases are made on the dark web is with digital currency, such as bitcoin, which is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. The network is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a block chain. Every bitcoin transaction that occurs in the entire payment network is recorded on the block chain.

13. Individuals store information about their bitcoin in a bitcoin virtual “wallet,” which acts as a bitcoin equivalent of a bank account. Bitcoin wallets have a private key and a public key, which is commonly known as the wallet address. Bitcoin wallets are electronic in nature and may be stored on mobile devices, external or removable media, or computers. In addition, individuals conducting business with bitcoins can back-up wallets to paper printouts, which would contain information to restore the wallet into an electronic form (this is known as cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. The keys are a series of alphanumeric characters that when used together will open a wallet and allow funds to be sent or received and can be provided to individuals who wish to consummate transactions with bitcoin. The public wallet address is recorded on the block chain when a transaction is processed. A single user can create hundreds of unique bitcoin addresses attached to a single bitcoin wallet. Bitcoin address clustering is a process that attempts to analyze these transactions and discover addresses generated by a single user or entity, then group them into what is known as a cluster that can be associated to a wallet. Bitcoin is pseudonymous, meaning that the digital currency is not tied to an identifiable real-world entity but rather to a bitcoin address. Owners of a bitcoin address are not explicitly identified and new addresses can be generated for every new transaction to increase anonymity.

14. After a transaction is complete and a dark web market vendor receives the cryptocurrency, the vendor has many options of what to do with the cryptocurrency. For example, the vendor can simply leave the cryptocurrency in the digital wallet linked to the dark web marketplace where the sale occurred, he can transfer it from that wallet to another digital wallet or application or software used for holding cryptocurrency, or he could transfer the cryptocurrency

to a peer or an exchange for the conversion of the cryptocurrency to actual, tangible currency such as United States currency.

15. The purchase and sale of bitcoin can be conducted either through an online exchange where the transaction occurs with the exchange, or through a peer-to-peer transaction that does not use an established exchanging service as an intermediary. Peer-to-peer transactions can be conducted anonymously from any location with an internet connection, or by individuals meeting in person where the seller sends bitcoin from their digital bitcoin wallet directly to a buyer's bitcoin wallet in exchange for a predetermined amount of fiat currency or other asset.

16. Individuals conducting business in this manner must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving bitcoin. Such devices are also necessary to access and conduct transactions on a dark web marketplace.

SUMMARY OF THE INVESTIGATION

17. Beginning in August 2019, and continuing until the present, a joint investigation commenced targeting the SSH comprised of the following law enforcement agencies: United States Postal Inspection Service (USPIS); Homeland Security Investigation (HSI); Houston Police Department.

18. The investigation has determined that beginning in approximately 2019, SSH, which included William Wells) operated an online drug trafficking organization responsible for the manufacturing and distribution of heroin, cocaine and methamphetamine to individuals throughout the United States. During this span, Wells based his operations in Houston, TX. SSH

operated online via various dark web marketplaces and a Wickr chat room. The two marketplace vendor accounts operated were, FIENDEMPIRE and HTRAIN, while the Wickr chat room operated was, deepdreamz.

CONTROLLED PURCHASES AND SEIZED PARCELS

19. Beginning in August 2019, I became aware of several U.S. Postal Service (USPS) parcels associated to this investigation that were identified to have been mailed at the Debra Sue Schatz Post Office, located at 2909 Rogerdale Rd Houston TX 77042. The Debra Sue Schatz Post Office is approximately 2.5 miles away from the Subject Location.

20. On October 21, 2019, Inspector Whitsitt conducted an undercover narcotics buy via the dark web app Wickr. Inspector Whitsitt used the moniker Forthefour to contact moniker deepdreamz. Deepdreamz is the wickr moniker assumed by dark web vendor STILLSKYHI (SSH). Dark web vendor STILLSKYHI has been identified as William Wells. Inspector Whitsitt purchased 3 grams of "#4 tan Heroin" from STILLSKYHI. The price of the Heroin was \$149.00 per gram and express shipping rate was \$49.00. Inspector Whitsitt transferred SSH .060547 Bitcoin to wallet address 141b2KxNdVpdrQo5P7JdcsBr5t6ePnDSEz for a total dollar value of \$469.69. SSH responded with "set." During the undercover purchase Inspector Whitsitt provided the mailing address of Brad Triofante PO Box 91188 Cleveland, OH 44101. This is an Inspection Service controlled Post Office Box utilized for the purpose of undercover narcotics purchases.

21. On October 22, 2019, HSI Houston Special Agents, Houston Postal Inspectors and Houston Police Department Sargent Mark Shoffner (a Task Force Officer with the HSI Houston IAH BEST) established surveillance around the suspected address of Wells/STILLSKYHI. At approximately 4:48 PM CST, WELLS departed the 4400 Boone Road Apt 144 in the 2016 Toyota Corolla bearing TX License Plate HXT-0869 and traveled to 11703

Beechnut St. Houston, TX 77072 (hereafter referred to as the Beechnut Post Office). WELLS arrived at Beechnut Post Office at 4:56 PM CST. Special Agent (SA) Robert Haberkamp witnessed WELLS enter the post office carrying a black bag as he entered the Post Office. Inspectors Grafmiller and Macdougall entered the Beechnut Post Office and observed Wells ship multiple Express Mail and Priority Mail parcels. Inspectors Grafmiller and Macdougall then collected all of the parcels mailed by WELLS including the parcel from the undercover purchase. The return information on the UC purchase was Moulin Noir at 10901 Filey Ln., Houston, TX 77013. The parcel had USPS tracking number EJ 161 171 620 US. Inspector Whitsitt seized the parcel related to the UC purchase. On October 23, 2019, Inspector Whitsitt searched the USPS parcel assigned tracking number EJ 161 171 620 US. During the search, Inspector Whitsitt discovered WELLS was attempting to mask the illegal contents of the parcel by repackaging the heroin multiple times to give it a more legitimate feel to those handling the parcel. The priority mail express envelope had a second priority mail envelope inside, which had a greeting card envelope and card inside. Inside the card was a Mylar sealed pouch inside, which had a zip lock type bag containing three grams of heroin inside. The zip lock bag had a "3" written on it in black ink, possibly a sharpie marker. The heroin and packaging were seized by Inspector Whitsitt.

22. On November 04, 2019, Inspector Whitsitt conducted an undercover buy of 3 grams heroin, 2 grams cocaine and 2 grams methamphetamine from dark web vendor William Wells (moniker SSH). Inspector Whitsitt contacted Wells via Wickr messaging app using the user name Forthefour. Wells utilizes moniker deepdreamz on wickr. Inspector Whitsitt sent .077771 Bitcoin with a US dollar value of \$732.00 to Wells wallet address 1Mi4JH7Hy9dVpqLqgapeBWHepUEfUhc1o for the narcotics and express mail shipping.

During the undercover purchase Inspector Whitsitt provided the mailing address of Brad Triofante, PO Box 91188, Cleveland, OH 44101. This is an Inspection Service controlled Post Office Box utilized for the purpose of undercover narcotics purchases. On November 5, 2019, Inspectors Whitsitt and Reyes, along with HSI conducted surveillance on Wells and observed him go to three different Post Offices and mail suspected narcotics parcels. Wells went to Debra Sue Schatz, Demoss and Houston Main Post Office. On November 6, 2019, Inspector Whitsitt contacted Wells (SSH) (deepdreamz) via Wickr as to the status of the narcotics purchased during the undercover purchase. Wells responded "set". Wells then shipped Express mail parcel with tracking number 9470136897846118810023, from the Memorial Park Post Office located at 10505 Town and Country Way, Houston, Texas 77024. The parcel was addressed to Brad Triofante, PO Box 91188, Cleveland, OH 44101 with return address of Francis Pergio, 6575 Highway 6 N Houston, Texas 77064-1311. On November 8, 2019, Express Mail parcel with tracking number 9470136897846118810023 was delivered to Post Office Box 91188, Cleveland, OH 77064-1311. Teresa Milite with the Postal Inspection Service in Cleveland, OH placed the unopened parcel into Express Mail parcel EJ047126896US and mailed it to Inspector Whitsitt, 4600 Aldine Bender Road, Room 400, Houston, TX 77315. On November 12, 2019, Inspector Whitsitt searched Express Mail parcel 9470136897846118810023. During the search, Inspector Whitsitt discovered WELLS was attempting to mask the illegal contents of the parcel by repackaging the heroin multiple times to give it a more legitimate feel to those handling the parcel. The express mail parcel contained a Priority Mail Express envelope and inside the Priority Mail Express envelope was a foam brown pumpkin covered in glitter. Inside the pumpkin was a red sealed Mylar container, which contained a clear heat sealed baggie. Inside the clear heat sealed baggie was three clear plastic baggies; one pink, one blue and one black. The

pink in color baggie had a number "2" written on the outside, and contained a white powdery substance that tested positive for cocaine. The blue in color baggie had a number "2" written on the outside, and contained a clear rock like substance that tested positive for methamphetamine. The black baggie had a number "3" written on the outside, and contained a tan powder substance that tested positive for heroin.

23. On November 25, 2019, HSI Agent Haberkamp deployed a surveillance vehicle to 4400 Boone Road, Houston TX, in order to record Wells leaving apartment 144 with a blue and black bag draped over his shoulder. This bag has been utilized many times by Wells to carry suspected narcotics parcel from his residence to the Post Office. On November 25, 2019, Inspector Whitsitt utilized the Wickr screen name Forthefour and made a UC purchase from William Wells (STILLSKYHI and Deepdreamz). Inspector Whitsitt purchased 10 grams of Heroin and provided the recipient information of Brad Triofante, PO Box 91188, Cleveland, OH 44101. Inspector Whitsitt transferred \$1531.00 (0.21355 BTC) to bitcoin address 1BauHaowBYDmePzcGAnA3wQS4XoJ15Y9g. On November 26, 2019, Inspectors Whitsitt and Reyes along with Houston Police Department Sgt. Mark Shoffner conducted surveillance on Wells in order to intercept the narcotics parcel Inspector Whitsitt had purchased from Wells the night before. At approximately 4:30 PM Inspectors Whitsitt, Reyes and HPD Sergeant Shoffner observed Wells leave apartment 144 carrying a large blue and black bag via the surveillance vehicle deployed at the location. Utilizing the vehicle tracker placed on Wells vehicle they followed Wells to the Debra Sue Schatz Post Office. At the post office, Wells shipped 21 suspected narcotics parcels including the one purchased by Inspector Whitsitt via Wickr on November 25, 2019. Inspector Whitsitt recovered Express Mail parcel with tracking number 9470 1368 9784 6161 9189 36. On November 27, 2019, Inspector Whitsitt in the presence of

Inspector Reyes opened Express Mail parcel 9470 1368 9784 6161 9189 36. The parcel was addressed to Brad Triofonte, PO Box 91188, Cleveland OH 44101-3188 with sender name Stephen Hirschst, 10210 Westheimer Road, Houston TX 77042-3116. During the search, Inspector Whitsitt discovered WELLS was attempting to mask the illegal contents of the parcel by repackaging the heroin multiple times to give it a more legitimate feel to those handling the parcel. Inside the Express Mail envelope there was a Priority Mail envelope with a number "4" sticker. Inside the priority mail envelope there was a greeting card with a red flower on in, which contained a plain white envelope. Inside the plain white envelope was a green heat sealed package, which contained a heat sealed clear plastic baggie that had two clear yellow baggies label with a "5". The contents of the two yellow baggie was a tan rock like substance believed to be heroin. The substance field tested positive for heroin in the presence of Inspectors Whitsitt and Reyes.

24. On December 17, 2019 Inspector Whitsitt at approximately 7:00 PM observed Phuong Thao Huynh mail suspected drug parcels from the Houston Mail Post Office. Huynh is the co-habitant and the name listed on the lease at 4400 Boone Road Apartment 144, she is also the registered owner of the 2016 Toyota Corolla with Texas License Plate HXT-0869.

25. On December 17, 2019 Inspector Whitsitt contacted STILLSKYHI/deepdreamz via wickr and initiated an undercover purchase of Heroin. Inspector Whitsitt utilized the Wickr profile of Forthefour and sent a message to deepdreamz asking if there were any specials. Deepdreamz responded that there is a currents special of 3.5 grams of Heroin for \$499.00 plus \$49.00 for express shipping. Inspector Whitsitt sent \$548.00 in Bitcoin (0.08217077) to wallet address 1P6pSrUCmAt3tTE9iF2d8nx2R7FZEPw3rD along with the shipping address of Brad Triofonte P.O. Box 91188 Cleveland, OH 44101. Deepdreamz responded with "set".

26. On December 18, 2019 Inspectors Whitsitt and Grafmiller, HSI agent Haberkamp and Houston Police Sergeant Shoffner conducted surveillance on Huynh. Utilizing the vehicle tracker that was placed on the 2016 Toyota Corolla with Texas license plate HXT-0869 we followed Huynh from her residence at 4400 Boone Road Apt 144 Houston Texas to the Houston Main Post Office located at 1500 Hadley Street Houston, Texas. Surveillance video inside the post office showed Huynh mailing 33 suspected drug parcels, including the one purchased by Inspector Whitsitt via Wickr on December 17, 2019. Inspector Whitsitt recovered Express mail parcel with tracking number 9270 1902 4167 5500 0000 3938 65. The parcel had the sender name of Stewart Kat 3201 Sacket Street Houston, TX 77098 and the receiver name as Brad Triofante P.O.91188 Cleveland OH 44101-3188.

27. On December 19, 2019 Inspector Whitsitt and Reyes opened Express mail parcel 9270 1902 4167 5500 0000 3938 65. During the search, Inspector Whitsitt discovered Huynh was attempting to mask the illegal contents of the parcel by repackaging the heroin multiple times to give it a more legitimate feel to those handling the parcel. Inside the Express Mail envelope there was a Priority Mail envelope. Inside the priority mail envelope there was a greeting card. Inside the greeting card was a green sealed package, which contained a heat sealed clear plastic baggie that had one clear black baggies label with a "3.5". The contents of the one black baggie was a tan rock like substance believed to be heroin.

28. On December 23, 2019 Inspector Joseph Macdougall, HSI agent Haberkamp and Houston Police Department Sergeant Shoffner conducted surveillance on Huynh. They observed Huynh leave her residence at 4400 Boone Road Apartment 144 Houston, TX in the 2016 Toyota Corolla with Texas License Plate HXT-0869 and drive to the John Dunlop post office located at 8728 Beverly Hill Street Houston, TX 77063. They observed her

mail 12 suspected narcotics parcels from this post office. Inspector Macdougall intercepted Express mail parcel with tracking number 9270 1902 4167 5500 0000 4106 16. Sergeant Shoffner then conducted a traffic stop on the 2016 Toyota Corolla with Texas License Plate HXT-0869 and positively identified Huynh as the driver and sole occupant of the vehicle.

29. On December 26, 2019 Inspector Whitsitt executed parcel search warrant number 4:19mj2397 on express mail parcel 9270 1902 4167 5500 0000 4106 16. This is the parcel that was mailed by Huynh on December 23, 2109. During the search, Inspector Whitsitt discovered Huynh was attempting to mask the illegal contents of the parcel by repackaging the heroin multiple times to give it a more legitimate feel to those handling the parcel. Inside the Express Mail envelope there was a Priority Mail envelope. Inside the priority mail envelope there was a yellow with white dot paper container. Inside the container was a red sealed package, which contained a heat sealed clear plastic baggie that had one clear black baggies label with a "4.5" and a clear pink bag labeled with a "1". The contents of the one black baggie was a tan rock like substance believed to be heroin. The rock like substance field tested positive for Heroin. The contents of the clear pink baggie was a white powdery like substance that field tested positive for cocaine.

30. On January 24, 2020, Department of Homeland Security Special Agent De La Fuente Jr. deployed a continuous surveillance vehicle to 4400 Boone Road with direct line of sight to apartment 144, the residence of Wells and Huynh. At Approximately 4:44 PM on January 24, 2020 Wells is observed leaving apartment 144 at 4400 Boone Road Houston, Texas and get into the 2016 Toyota Corolla bearing Texas License plate HXT-0869. Wells was carrying the blue and black bag that he and Huynh have both used on previous occasions to carry parcels contained narcotics. The black and blue bag appeared to be filled with parcels. The

vehicle tracker shows Wells leave this location and go directly to the Beechnut Post Office arriving at approximately 4:53PM. Wells returned to the residence at approximately 5:28 PM carrying the black and blue bag which appeared to be empty.

31. Inspectors and Agents have conducted surveillance on Wells and Huynh on multiple occasions beginning in October 2019 to January 2020. This surveillance has been conducted for both controlled buys that have been made from SSH and to gather information regarding the mailing of narcotics. In each of these instances that narcotics have been seized from parcels mailed via the United States Mail Inspectors and Agents have observed either Wells or Huynh leave 4400 Boone Road Apartment 144 and get into the 2016 Toyota Corolla bearing Texas License Plate HXT-0869 and drive to various post offices throughout the Houston area. The residence also has multiple surveillance cameras facing the parking lot and the front door. This behavior is not common for this apartment complex, however this is common for individuals who are engaging in illegal activity. Inspectors and Agents believe this is the location where Wells and Huynh are operating the dark web criminal enterprise of STILLSKHI, from accepting orders and payments, weighing and packaging drugs and preparing narcotics parcels to be distributed via the United States Mail.

32. Phuong Thao Huynh is the registered lease holder of this apartment and Wells has received several parcels addressed to him at this address including one as recent as January 25, 2020.

THE SUBJECT LOCATION

1. Based on my experience and training, continued consultation with other Postal Inspectors and other law enforcement officers experienced in drug and financial investigations, and the facts set forth herein, I believe that the property to be seized, as set forth in Attachment B,

will be found in the location to be searched, as described in Attachment A, for the following reasons:

a. Individuals involved in drug dealing often maintain in their residences or vehicles records and ledgers evidencing their trafficking activities in order to keep track of the ordering purchasing, storage, distribution, and transportation of controlled substances. On numerous occasions, I have observed handwritten notes which depict drug transactions in pay-and-owe records and in customer lists complete with telephone numbers and addresses. These records, which remain to memorialize past transactions and track the status of accounts receivable and accounts payable, are kept whether or not the individual is in actual possession of controlled substances or currency at any given moment.

b. Individuals involved in drug dealing will use their cellular telephones or computers to conduct the drug trafficking business. Often stored in the telephones' or computers' memory are contact names, telephone numbers, recent calls, text messages containing addresses and tracking numbers for parcels and other transactions, internet history, and photographs which are related to controlled substance trafficking. This is particularly so in a case like the instant investigation where the DTO is known to sell narcotics and launder money using the internet.

c. Individuals involved in drug dealing earn large sums of money and/or virtual or cryptocurrency currency and often try to legitimize these profits. In order to do this, they may attempt to secrete, transfer, and conceal the money in several ways, including, but not limited to, the following: (1) placing assets in names other than their own to avoid detection while maintaining control of the assets, (2) laundering the money through what appears to be a legitimate business, (3) hiding the money in their homes, safes, and safety deposit boxes, (4) using the money to buy assets which are hard to trace, or (5) transferring assets into what appear to be legitimate

amounts, to other individuals. Records of these transactions including banking records are often found in drug dealers' residences. In addition, as described in this affidavit, individuals who sell drugs for bitcoin often use sites like localbitcoins.com to convert their proceeds to fiat currency, or use sites like Gyft to convert their proceeds to gift cards that can be spent on goods and services.

d. Individuals involved in drug trafficking must maintain on hand large amounts of United States currency and/or virtual currency in order to maintain and finance their on-going drug business. In addition, other assets generated by their drug business or purchased with the cash earned such as jewelry and negotiable/financial instruments, are typically kept by drug dealers within their residences or vehicles to avoid detection by law enforcement.

e. It is common for drug traffickers to maintain in their residences drug paraphernalia relating to the sales and distribution of controlled substances, such as plastic baggies, zip-lock baggies, cellophane and other items used for the weighing, packaging, and distribution of controlled substances for sales. These items are also commonly found in places where controlled substances are being stored and or prepared for shipment through the U.S. Mail and other private commercial carrier systems.

f. Individuals involved in the distribution and sale of controlled substances commonly possess, carry, or keep firearms and other weapons in order to protect their drugs and drug-related proceeds from discovery, theft by criminals, or confiscation by law enforcement.

g. Individuals involved in the distribution and sale of controlled substances commonly utilize their vehicles as an integral part of their illegal enterprise. Such uses include counter surveillance, the delivery of the drugs for sale, transportation of supplies and equipment necessary for the sale of the drug, packaging of the drug, protection of the drug, storage of the drugs, and as an asset for concealing the profits of their drug business. In addition, persons

involved in the trafficking of controlled substances often travel by other means, to include airplane, to conduct their business and keep travel records and receipts and used airline tickets.

h. Individuals involved in drug dealing often take, or cause to be taken, photographs of themselves and their associates, their property and their drugs, and these individuals usually maintain these photographs in their possession. This is especially true when the drugs are, like in this case, advertised for sale online.

i. Within any location searched there will often be keys that fit location locks, post office boxes, safe deposit boxes, commercial mailing receiving agency boxes, wallets, purses, diaries and luggage tags, all of which contain some personalization that tends to identify the owners, thus tending to establish the identity of persons in control of the premises, vehicles, storage areas or containers where evidence of controlled substance trafficking may be found, including utility company receipts, rental receipts, and canceled mail envelopes. In virtually all locations that I have searched, I have observed utility bills pertaining to the location, and personal letters addressed to occupants of the location.

j. Further, in my experience, narcotics traffickers are not unlike any other individual in our society in that they maintain documents and records. These documents and records will normally be retained for long periods of time regardless of whether their value to the individual has diminished. Often times, this type of evidence is generated, maintained, and subsequently forgotten. Hence, records that one would normally think a prudent person would destroy because of their incriminating nature of the documents, they keep. The documentary evidence most commonly seized includes telephone numbers, address books, credit cards and hotel receipts documenting travel, mobile telephone records, accounts and records in fictitious names, carbon copies of money orders and cashier's checks evidencing large cash expenditures,

correspondence, and records indicating the existence of storage facilities used in narcotic trafficking. This evidence is more and more frequently found in electronic format. People conduct the ordinary affairs of life, whether making travel plans or business arrangements, using computers and electronic devices such as smart phones that operate as computers.

k. Finally, I am aware that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime; and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data).

SEIZURE AND SEARCH OF COMPUTERS

2. In this affidavit, the terms “computers” or “digital storage media” or “digital storage devices” may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

3. As described above and in Attachment B, I submit that if computers or storage media are found at the Subject Location, there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. I am aware that

modern cellular telephones, or smart phones, operate in many respects as a computer, with internet access, and function at times as a person's computer historically would have.

4. Based on my own, and my colleagues' knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks, and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

5. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

6. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic

evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

7. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when they were used.

8. The monitor and printer are also essential to show the nature and quality of the images or files that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the

seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

9. The computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used as instrumentalities of the crime to operate the computer to commit the offenses discussed in this affidavit. Devices such as modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet or to otherwise commit the crimes described herein. The computer equipment may also have fingerprints on them indicating the user of the computer and its components.

10. Similarly, information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

11. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example,

registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

12. I know from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

13. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by “hiding” files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for

by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

14. For example, the search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following on-site techniques (the following is a non-exclusive list, as other on-site search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when, and may contain information about encryption, virtual machine software (virtual operating systems that are lost if the computer is powered down or encrypted);

c. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for any examination.

15. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how, when and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

b. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

e. Need to review evidence over time and to maintain entirety of evidence. Your Affiant recognizes the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. Your Affiant advises it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. Your Affiant has learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated

data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, your Affiant has reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. Your affiant has learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, your Affiant respectfully requests the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated

examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

17. I know from training and experience that digital storage devices can be very large in capacity, yet very small in physical size. Additionally, I know from training and experience that those who are in possession of such devices also tend to keep them on their persons, especially when they may contain contraband or other evidence of a crime. The storage capacity of such devices can be as large as tens of gigabytes in size as further described below, which allows for the storage of thousands of images and videos as well as other digital information such as calendars, contact lists, programs and text documents. Such storage devices can be smaller than a postage stamp in size, which allows them to be easily hidden in a person's pocket.

18. I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the crimes described in this affidavit to include credit card bills, utility bills, mail, correspondence, and other identification documents.

19. I know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include identification documents, bills, and receipts.

20. When searching the Subject Location, Apple brand devices, such as iPad or iPhones, which are ubiquitous, may be found. Touch ID is a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button

on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, if the device is equipped with an operating system that is earlier than version 9.3, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. If the operating system is version 9.3 or later, that time frame shrinks to 8 hours. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to any Apple devices found at the Subject Location while executing the search warrant. The government may not be able to obtain the contents of the Apple devices if those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

21. In addition, I know in my training and experience that many other mobile device manufactures have their own version of Touch ID—that is, a fingerprint recognition feature that

the device's user can program and use to unlock the device. For instance, I know that Google Pixel phones and Google Pixel XL phones have a fingerprint sensor that can be used to unlock the device. Similarly, Samsung, LG, HTC, and other manufacturers also have devices with fingerprint sensors.

22. Similarly, in my training and experience I know that some applications loaded onto mobile devices or other electronic devices may be secured by the user with a thumbprint or fingerprint. Common among these types of applications are applications such as mobile banking apps or other financial applications, password storage applications, and secure communications apps, among others.

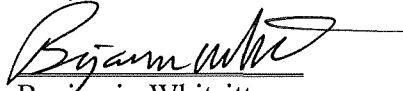
23. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the Subject Location to the Touch ID sensor or other device fingerprint sensor of the seized device, to the extent a visual inspection of those devices reveals that the device has a fingerprint sensor—located pursuant to the warrants requested by this Affidavit for the purpose of attempting to unlock the device via Touch ID or other fingerprint sensor in order to search the contents (including applications) as authorized by this warrant.

24. Furthermore, for the reasons set forth below, I submit belief that sufficient probable cause has been established to search and seize any online black market vendor accounts, online digital currency exchange platform accounts, and the data contained therein. Due to the inherent illicit and anonymous nature of these accounts, and that there is no identified service provider for these accounts, legitimate, compliant or not, to which legal process may be served; your affiant believes this to be the only manner to recover said evidence.

CONCLUSION

25. Based on the above facts, I believe there is probable cause to believe that Wells is engaged in violations of the Subject Offenses, and fruits and items used in furtherance of those offenses, as specified in Attachment B of this affidavit, are located at the locations described in Attachments A of this affidavit.

I, Benjamin Whitsitt, an agent with the United States Postal Inspection Service, being duly sworn according to law, hereby state that the facts stated in the foregoing affidavit are true and correct to the best of my knowledge, information, and belief.


Benjamin Whitsitt
United States Postal Inspector

Sworn and Subscribed to me telephonically this 29th day of January 2020, and I find probable cause.


UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF TEXAS

This Application and Affidavit was reviewed and submitted by AUSA Celia Moyer.